Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1 – 4. (canceled)

5. (currently amended) A method of protecting at least one electronic component of a product against illicit manipulation and/or unauthorized access, characterized by the following method steps:

(i) checking that at least one activation ~~activating~~ condition is met by means of at least one activating unit,

(ii) if at least one activation condition is met, recognition of this fact and the desired effects it is to have are placed in store in coded form in at least one memory element that is used for starting-up the component, and

at the next attempt to start up the product;

reading out the activation condition; ~~in the event of illicit manipulation of the component and/or unauthorized access to the component activating at least one preventing unit that is connected to the activating unit,~~ and

(iii) in response to the activation condition, activating at least one preventing unit that is connected to the activating unit and at least partly de-activating the operation of the component and/or at least partly destroying the component, by means of the preventing unit;

characterized in that the at least partial de-activation of the operation of the component and/or the at least partial destruction of the component is carried out during the start-up of the product by

(j=1) preventing an internal oscillator from beginning to oscillate;

(j=2) preventing an oscillator for an external clock signal from beginning to oscillate;

(j=4) preventing the build-up of a high voltage; and

(j=7) switching on an increased current drain in the operating state or the quiescent state.

6. (currently amended) A method as claimed in claim 5, characterized in the check on whether the activation ~~activating~~ condition is met is made by analyzing at least one data stream applied from outside or by signals from the internal sensor circuitry of the component.

7. (canceled)

8. (previously presented) A method as claimed in claim 5, characterized in that the activation takes place

(i=1) as a result of the recognition once or more than once of at least one illicit command,

(i=2) as a result of the recognition of a multiplicity of different illicit operations,

(i=3) as a result of the issue of at least one specific activating command,

(i=4) as a result of the issue of at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i=5) as a result of the recognition once or more than once of at least one physical attack on the component, by means of sensor circuitry belonging to the component that is intended for this purpose.

9. (previously presented) A method as claimed in claim 5, characterized in that the at least partial de-activation of the operation of the component and/or the at least partial destruction of the component is carried out by

(j=3) switching off a high-voltage limiter, in particular by means of permanent programming,

(j=5) reprogramming the allocation of addresses and/or the allocation of data, and/or

(j=6) loading at least one memory element of the component with illicit values of data.

10. (canceled)

11. (canceled)

12. (canceled)

13. (currently amended) A method of protecting at least one electronic component of a product against illicit manipulation and/or unauthorized access, characterized by the following method steps:

checking that at least one activation ~~activating~~ condition is met by means of at least one activating unit,

if at least one activation condition is met, recognition of this fact and the desired effects it is to have are placed in store in coded form in at least one memory element that is used for starting-up the product~~component~~, and

at the next attempt to start up the product;

reading out the activation condition; and

at least partly de-activating the operation of the electronic component and/or at least partly destroying the electronic component, by means of a preventing unit;

characterized in that the at least partial de-activation of the operation of the component and/or the at least partial destruction of the component is carried out during the start-up of the product by;

switching on an increased current drain;

blocking generation of high voltage;

ignoring an external clock signal; and

stopping an internal clock signal.

14. (currently amended) A method as claimed in claim 13, characterized in that the check on whether the activation ~~activating~~ condition is met is made by analyzing at least one

data stream applied from outside or by signals from the internal sensor circuitry of the component.

15. (previously presented) A method as claimed in claim 13, characterized in that the activation takes place

(i=1) as a result of the recognition once or more than once of at least one illicit command,

(i=2) as a result of the recognition of a multiplicity of different illicit operations,

(i=3) as a result of the issue of at least one specific activating command,

(i=4) as a result of the issue of at least one activating command together with data that addresses a plurality of components by means of at least one group coding, or an individually coded component, and/or

(i=5) as a result of the recognition once or more than once of at least one physical attack on the component, by means of sensor circuitry belonging to the component that is intended for this purpose.